

# I3P Task 5 CDIS Gap Analysis

**Timothy Draelos and Annie McIntyre**  
Sandia national Laboratories<sup>1</sup>

**Michelle Gosseline and Chris Eliopoulos**  
The MIRE Corporation  
March 13, 2006

---

<sup>1</sup> Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under Contract DE-AC04-94AL85000

This work was supported under grant number 2003-TK-TX-0003 from the U.S. Department of Homeland Security, Science and Technology Directorate. Points of view in this document are those of the author(s) and do not necessarily represent the official position of the U.S. Department of Homeland Security or the Science and Technology. The I3P is managed by Dartmouth College.

---

## TABLE OF CONTENTS

---

EXECUTIVE SUMMARY .....	3
1. Introduction .....	4
2. What is CDIS? .....	4
2.1 Business LAN to Control Center LAN .....	5
2.2 PCS Community Members and Government Agencies .....	5
2.3 Among Members of the PCS Community .....	6
3. Why is CDIS Necessary? .....	6
4. Known Gaps to a CDIS Solution for Sector Use .....	7
4.1 Control of Shared Information .....	7
4.2 Vendor Participation .....	8
4.3 Anonymous Authentication .....	8
4.4 Access Control to Data .....	8
4.5 Analysis Capability .....	8
4.6 Summary of Technical Gaps and Requirements .....	9
5. Components of a CDIS Solution .....	10
5.1 Secure Databases .....	11
5.2 Interactive Web Capabilities .....	12
5.3 Links to Government .....	12
6. Summary .....	12
7. References .....	13

---

## TABLE OF FIGURES

---

Figure 1: Examples of information sharing across domains .....	4
Figure 2: Industry Requirements and Gap Analysis .....	9
Figure 3: Logical Layout and Flow of Information .....	10
Figure 4: Example Use Scenario for CDIS .....	11

---

## EXECUTIVE SUMMARY

---

I3P Task 5 addresses cross-domain information sharing among the oil and gas sectors. A visible industry consensus illustrates a recognized need to share information at various levels and among various stakeholders of the industry. Cross-domain information sharing (CDIS) provides a means to securely share information among industry asset owners and vendors. Any information that can be used to prevent, recognize, and mitigate an attack on infrastructure systems proves valuable. A comprehensive CDIS design will best identify and address coordinated attacks on the oil and gas sector, and contribute to the identification of coordinated attacks on the national critical infrastructure. Knowledge gathered from industry at the I3P workshop in June, 2005 and in subsequent forums and surveys has provided the Task 5 team with the following set of requirements for information sharing in this industry.

- User anonymity with authentication
- Sharing of various types of data (best practices data, incident information, system status, surveillance data, and reference information)
- Alerting
- Controlled access to shared information
- Analysis capabilities

Gaps identified in current information sharing solutions include the ability to provide anonymous yet authenticated communication, an automated and interactive analysis capability, controlled access to shared information, and a searchable database of incident information with forensic data and attack details. A CDIS design was developed by the Task 5 team to bridge the existing gaps in capabilities and technology and enable the sharing of information across various sectors of a user community. A CDIS proof-of-concept is being developed by the I3P team, demonstrating a subset of overall requirements and addressing specific, identified gaps. This proof-of-concept will facilitate anonymous reporting of critical incident information by authenticated members of the asset owner and vendor community, analysis and storage of that information, and communication of analysis output back to the user community. Information will be shared based on releasability rules and protected from unauthorized access or disclosure.

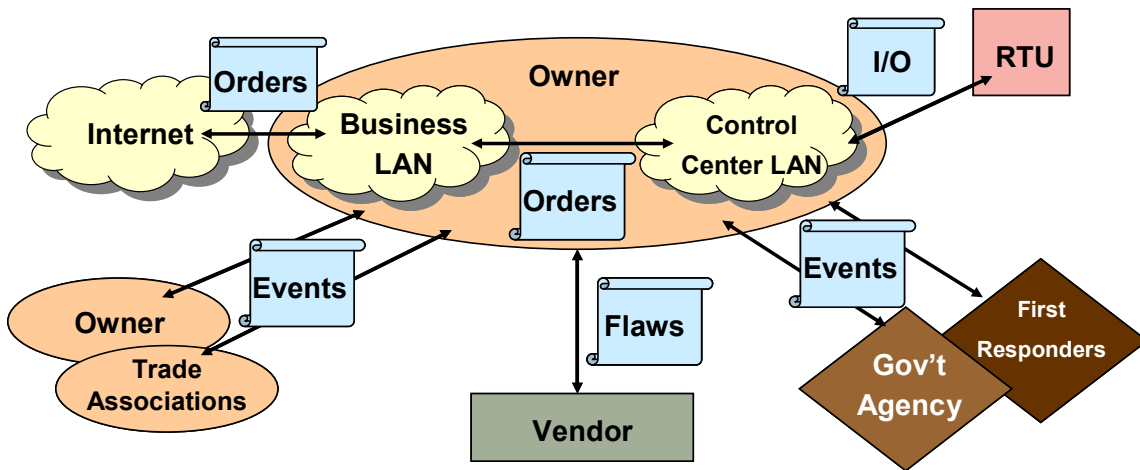
# 1. Introduction

I3P Task 5 addresses cross-domain information sharing among the oil and gas sectors. Reviewing industry forum data, references from the I3P workshop, and points from stakeholder discussions, a recognized need exists to share information at various levels and among various stakeholders of the industry. This white paper identifies important gaps between existing cross-domain information sharing capabilities and our view of the needed CDIS solution. Although other gaps may exist in the domain, we focus on the most critical gaps identified by industry and control systems researchers. We conclude with a vision of what a CDIS system should look like and how it should operate.

# 2. What is CDIS?

Cross-domain information sharing, in this context, is the exchange of information between two or more domains where a domain is a collection of individuals, resources, and information owned by one entity (e.g., company) that requires protection from other domains. Figure 1 below depicts the various cross-domain environments within the oil and gas community. Cross-domain information sharing within the oil and gas industry can be categorized in one of three ways:

- Business LAN to control center LAN information sharing,
- Information sharing between Process Control Systems (PCS) community members and government agencies, and
- Information sharing among members of the PCS community.



**Figure 1: Examples of information sharing across domains**

All of these CDIS categories are briefly described below and requirements for each are identified in [1]. However, the focus of our CDIS solution is on the problem of information sharing among members of the PCS community.

## **2.1 Business LAN to Control Center LAN**

Many owners feel that the risk associated with information sharing that takes place between the business LAN and the control center LAN is acceptable and additional security solutions are not required. To reduce the risk of sharing information between these two domains, additional information security controls, such as the use of information guards, could be integrated. Information guard solutions are available with varying features, including the ability to limit or control information flows between domains. Commercially available information guards would require tailoring to monitor and filter the specific data exchanged between the business LAN and the control center LAN.

## **2.2 PCS Community Members and Government Agencies**

Many owners feel that existing information sharing solutions for information flows from the owners to government agencies are sufficient. This information flow is regulated and procedures are in place to satisfy regulated reporting. Owners, however, would like to see more information flow from government agencies back to the owners. Government-hosted sites exist, or are being piloted, that provide general information to owners, including industry-wide alerts. Several of these sites are outlined below.

### **Homeland Security Information Network (HSIN)**

This network, hosted by the Department of Homeland Security (DHS), incorporates subsystems for critical infrastructure, oil and gas, and chemical security. The HSIN for critical infrastructure, or HSIN-CI, includes information exchanged between DHS and private sector owners and operators. Still in the pilot phase, geographic regions included in this network are Dallas, Atlanta, Seattle, and Indianapolis. The HSIN-CI pilot is an unclassified network that provides the DHS Operations Center with one-stop 24/7 access to the industry's broad information spectrum. It also facilitates two-way information sharing, providing DHS with a base of locally knowledgeable experts and delivers real-time access to needed information. It is accessed by locally vetted membership, and sends alerts via wired and wireless phones, email, fax, and pagers. HSIN-CI links into the FBI Tips program. Any information that is submitted via the Tips link is automatically transmitted to DHS and FBI headquarters for processing.

### **US-CERT®**

The US-CERT® offers alerts, tips, bulletins, and incident response services. The US-CERT® serves as a center for response to major incidents, fosters industry, government, and law enforcement collaboration, and hosts protection working groups, among other vulnerability reporting capabilities and training. Specifically, the Control Systems Security Center (CSSC) offers standards development, best practices, industry outreach, risk assessment methodologies, and vendor points of contact.

## **Infrastructure, Security, and Energy Restoration (ISER)**

The ISER site is hosted by the Department of Energy (DOE). It contains news, emergency situation reports, lessons learned, weather watch capabilities, preparedness plans, and links to government offices, trade associations, and other industry organizations. This new site encompasses information about natural disasters and emergency preparedness with a broader scope than data sharing for network attacks.

## **Energy Information Sharing Analysis Center (ISAC)**

The Energy ISAC site provided security related information sharing for the oil and gas and other critical infrastructure sectors by interfacing with relevant agencies such as DHS and DOE through coordinating councils. The ISAC site was previously maintained by Science Applications International Corporation (SAIC), but it is no longer operational.

### ***2.3 Among Members of the PCS Community***

The need that emerged as most pressing from discussions with key oil and gas stakeholders was the need for information sharing among members of the community. For example, shared data could provide base information for an organization to use in determining if it is under attack. Likewise, if other organizations report issues, this may be an indication that a coordinated infrastructure attack is underway. Attack and forensic data can be shared among members of the community and data can be analyzed to determine whether an infrastructure-wide attack is underway.

## **3. Why is CDIS Necessary?**

Today, information sharing must be viewed as a tool to protect assets and ensure uninterrupted operations and service. The I3P Task 1 Risk Characterization white paper [2] discusses threats and vulnerabilities to PCS systems, and their impacts on the overall business. Any information that can be used to prevent, recognize, and mitigate an attack on infrastructure systems proves valuable. As is discussed in the Risk Characterization white paper, the cost of inaction can be much greater in terms of downtime, public confidence levels, and equipment repair, than the costs of prevention and secure operations. The main objective of information sharing is to provide industry with the needed information to protect against, become aware of, and respond to threats. These threats can include overarching cyber, personnel, and physical security threats that can manifest as network attacks, software anomalies, and attempts at physical intrusion or gaining information. CDIS provides a means to share valuable types of information among industry asset owners and vendors that could help prevent, detect, or counter these threats. The types of information that could be shared via the CDIS include the following.

- Responses and Solutions
  - Alerts
  - Preparedness

- Protection
- Lessons learned
- Secure configurations
- Forensics
- Best practices
- Vendor information
- Incident information
  - Recent attacks
  - Effects
  - Actions
  - Areas affected
- System status
  - State of operations
  - Equipment failures and solutions
  - Outages
- Surveillance information
- Reference area
  - Links for regulations
  - Industry user group information
  - Assistance/incident response
  - DOE
  - DHS
  - Links to Government alerts

## **4. Known Gaps to a CDIS Solution for Sector Use**

There are a number of gaps that must be addressed in order to provide a CDIS solution to meet the requirements for information sharing within the oil and gas sector as described in [1]. Although others may exist, the most critical gaps identified by industry members and through research by the team are addressed. These gaps, discussed below, include how the site functions and critical capabilities provided to the user.

### ***4.1 Control of Shared Information***

Of primary interest to stakeholders is limiting who sees shared information inside and outside the industry. There currently is no developed, industry-only location for sharing all of the data types listed above. Industry stakeholders are adamant about creating an industry-only solution that includes controlled access and no government control. It would be recommended that a proposed CDIS solution be hosted within an industry organization with vetted membership and no government regulation. The data housed by this CDIS solution is then generated by asset owners/operators and vendors for use by this same community. This provides a single location for industry information and could serve as a jump point to government networks and resources. An industry operated site also stands the best chance of attracting and maintaining an active membership. A

CDIS solution could offer links to reporting alerts and obtaining government alert information from DHS and other sites to protect the national critical infrastructure.

## ***4.2 Vendor Participation***

Vendor participation has been suggested and recommended by numerous industry stakeholders. Receipt of anomaly data, critical failures within software, and the influx of user calls often make vendors the first point of aggregated identification of major security vulnerabilities, attacks, and implementation problems. Use of a CDIS system may allow proactive vendors to enlarge their customer base and to develop and implement secure infrastructure systems.

## ***4.3 Anonymous Authentication***

A security requirement consistently communicated by industry stakeholders is anonymity of information providers. The lack of an option for anonymous communication tends to suppress information sharing among competitors and industry participants. Requirements for a comprehensive CDIS design suggest incorporating anonymous, authenticated information sharing. Since anonymity can open the door for undetectable system abuse, revocable anonymity features should also be considered.

Capabilities exist in the commercial market today that provide anonymous web surfing, IP number masking, and other similar shields. However, anonymous authentication of users and anonymous submission of data from a trusted group has not been addressed. A technology developed at Sandia National Laboratories can be employed to fill this gap and provide the required anonymity that industry desires [3].

## ***4.4 Access Control to Data***

Owners are concerned about and want the ability to control the releasability of data that they share. Some data is appropriate to share with the entire sector while the sharing of other data should be restricted to certain sector members. A taxonomy for releasability needs to be defined and releasability rules need to be implemented.

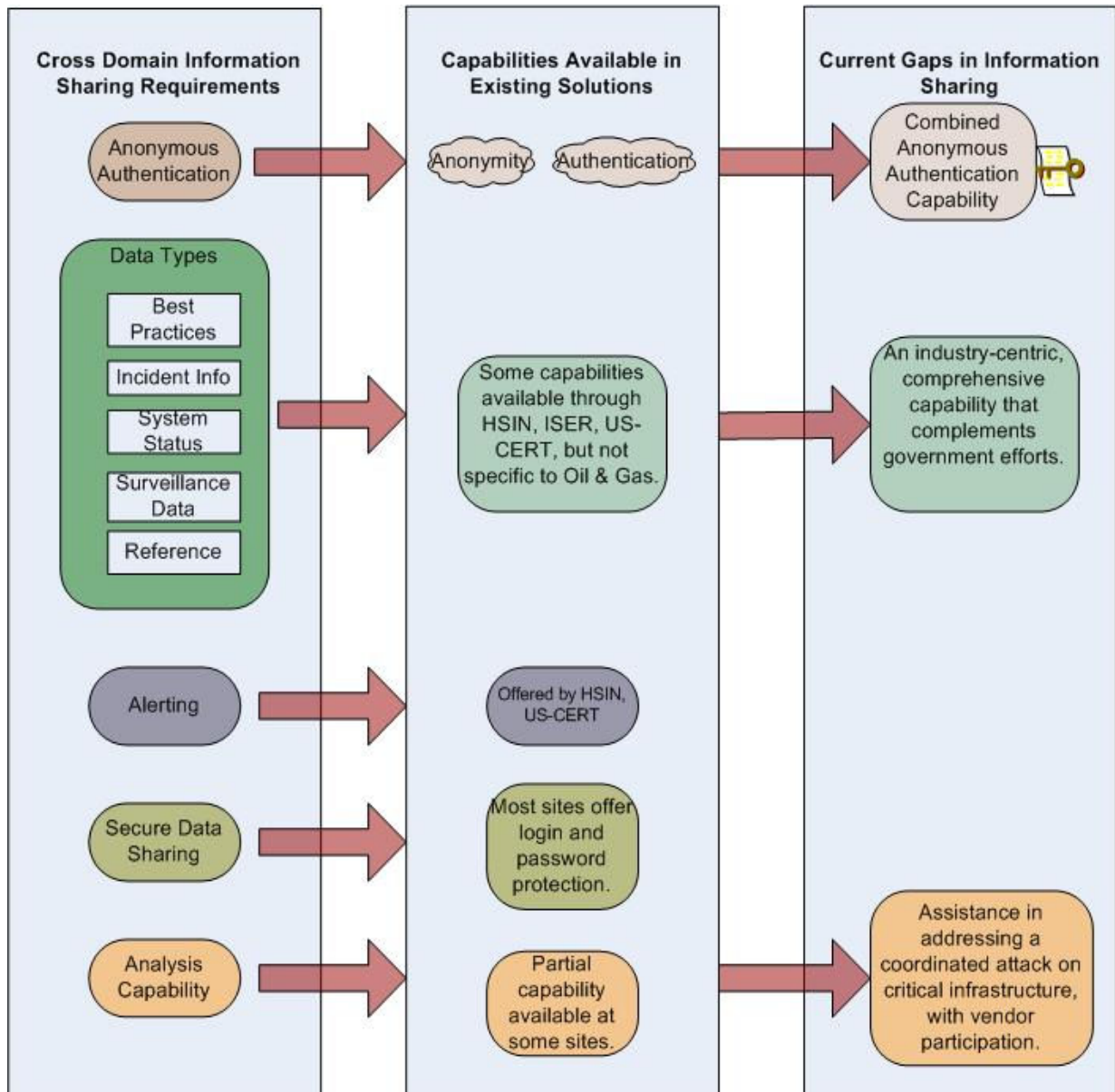
## ***4.5 Analysis Capability***

A CDIS system must be comprehensive but easy to use. A complete system should allow for the capture of incident information, forensic data, and surveillance data in searchable databases, allowing automated detection of coordinated attacks and providing an analysis mechanism for users. Across the sector, there is currently no standard analysis process or standard technology utilized by industry to derive information on attacks. Analysis processes are often unique to each organization and to each incident that occurs. The ability for a vendor or asset owner to analyze their information, especially time-sensitive data, may help mitigate immediate risks and stop an attack. One primary value of true cross-domain sharing of information is the aggregation of incident

information and the subsequent potential to detect coordinated, multi-site attacks. Detection of this kind will almost certainly require the use of computational analysis engines. A comprehensive CDIS solution should include both the ability for an asset owner or vendor to analyze his own activity as well as an overall automated analysis capability to correlate coordinated attacks on infrastructure. Links to government sites, alerts, and guidelines could be included, but shared data must stay within the CDIS system, avoiding FOIA issues and access outside the industry.

#### 4.6 Summary of Technical Gaps and Requirements

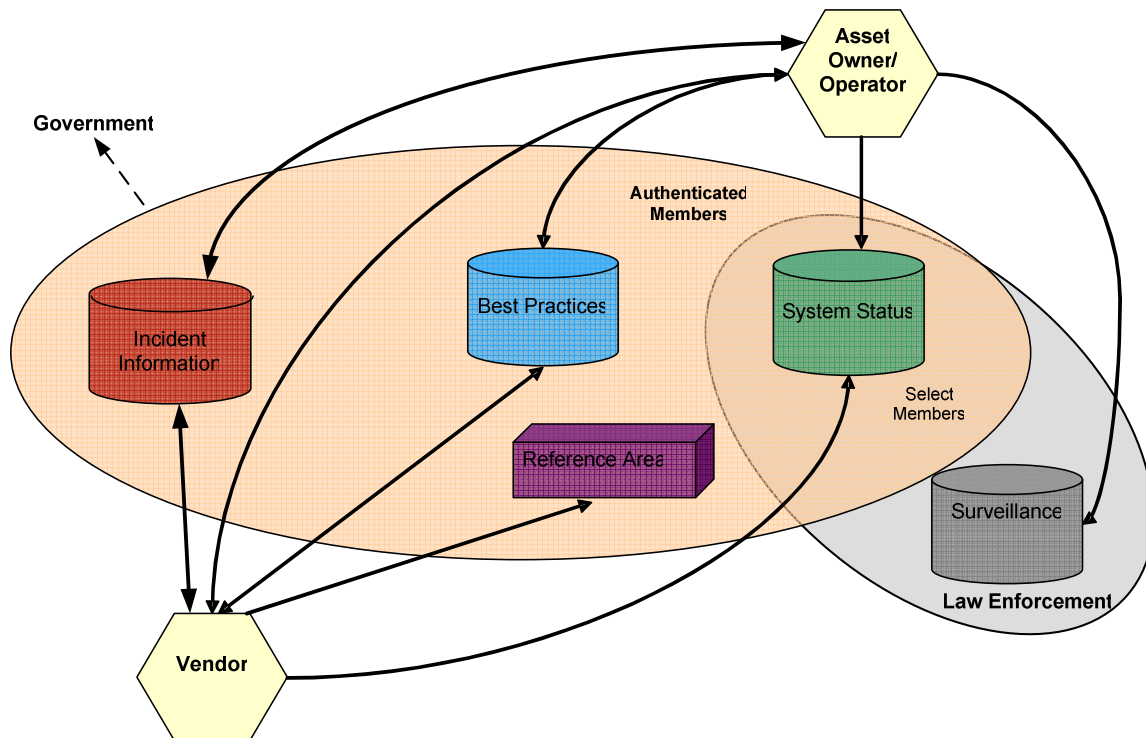
Figure 2 below illustrates existing gaps and industry requirements.



**Figure 2: Industry Requirements and Gap Analysis**

## 5. Components of a CDIS Solution

Initial gap analysis research found that a comprehensive solution with the required security controls did not exist as a whole in the commercial market. A CDIS design is proposed to address the sharing of information across various sectors of a user community, bringing together a variety of information in one virtual location, accessible only to authenticated members. Ideally, a complete CDIS design addresses all critical gaps. The proof-of-concept mentioned in earlier sections does not address all gaps nor does it include all functionality encompassed in the comprehensive CDIS design. A logical view of this proposed comprehensive design is seen in Figure 3.

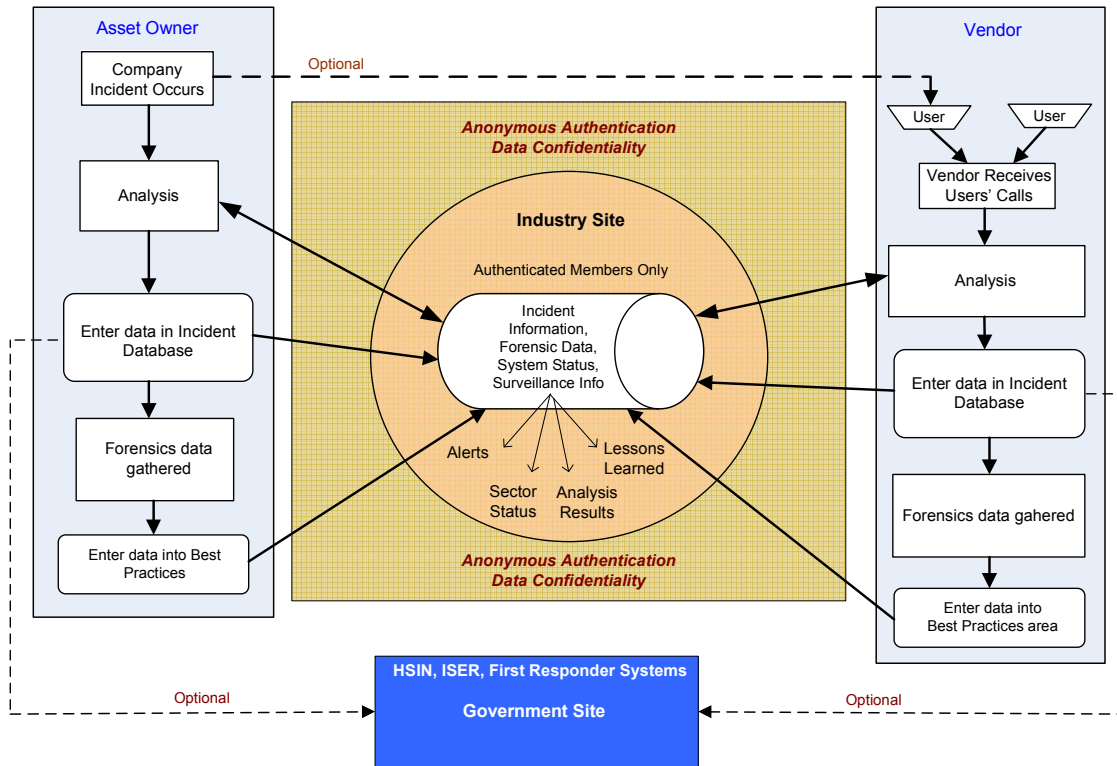


**Figure 3: Logical Layout and Flow of Information**

The design proposal suggests sharing this data among an industry group with vetted membership. This includes asset owners, managers, IT personnel, and vendors, who are often the first group to handle user calls and recognize network anomalies and attacks. This design may be the best way to determine and address a coordinated attack on the oil and gas sectors.

It is assumed that if the proposed CDIS system is accepted by industry, COTS technology pieces will be implemented with specialized development kept to a minimum and a there will be a focus on security. Figure 4 shows details of what a CDIS solution might look like with flow of information for an example attack

scenario. Each area of technology is discussed separately and mapped to areas within the CDIS system.



**Figure 4: Example Use Scenario for CDIS**

The structure of the proposed CDIS system includes secure databases, interactive web capabilities, and secure design and maintenance. Overall system and data security is addressed throughout the design.

### 5.1 Secure Databases

An advanced query capability should serve as an authorized user's main interface to information about incidents that have been reported. The ability to search for individual incidents and receive Data results of incident analysis and correlation provide users with improved situational awareness. These situations could be attacks, reconnaissance attempts, intelligence gathering, or system hijackings for use in a coordinated attack on an infrastructure.

An incident area that contains time-sensitive details of attacks on PCS systems and infrastructure support systems should be available. Information input to the CDIS system will be gathered via the use of online forms. Existing models for forms handling such information will be utilized if possible. Submission of the data will be performed using anonymous authentication and standard data security measures of data confidentiality and integrity. This technology will allow

data to be shared anonymously but with confidence that the data was provided from an authorized member of the community.

## **5.2 Interactive Web Capabilities**

Interactive tools that are commercially available such as forensic tools, data analyzers, and links to security tools, are currently being researched and will be integrated into the CDIS system as applicable.

## **5.3 Links to Government**

The government sites addressed in Section 2.2 can be linked to the CDIS system. Industry has the option to utilize government capability through links provided to these sites for alerts, standards, and other functionality. The CDIS system maintains an industry focus, however, as recommended by industry stakeholders. Each of these sites provides different functionality and our CDIS solution can fill industry gaps in information sharing while complementing government efforts.

## **6. Summary**

Data and knowledge from industry gathered at the I3P workshop and subsequent forums indicates a need for information sharing within the oil and gas industry. This information sharing capability must meet industry requirements, including the ability to provide an industry-only focus, anonymous data sharing, usability, and value of analyzed information available from a CDIS site. Main gaps identified include the ability to authenticate users and submit data anonymously, sharing of critical data types (incident information, system status, and surveillance data), and an automated analysis capability through a database of incident information, forensic data, and attack details. Other requirements include vendor participation and an industry-centric approach.

A CDIS design has been developed to meet industry needs. It is suggested that the CDIS system be hosted by an industry organization with vetted membership. Individual functional areas proposed include incident information, forensic data, and analysis tools. Standard security controls will be applied to information into, out of, and within the system to provide data confidentiality and integrity as needed. In addition, anonymous authentication capabilities for data submission will be leveraged from prior research. This capability can be matured and implemented within the CDIS system to meet industry needs. Such a comprehensive CDIS design will help identify and address coordinated attacks on the oil and gas sector, and contribute to the identification of coordinated attacks on the national critical infrastructure.

## **7. References**

- [1] J. Watters and C. Eliopoulos, "Requirements for Cross-domain Information Sharing Within SCADA Environments," I3P Research Report. 2005.
- [2] A. McIntyre, J. Stamp and A. Lanzone, "I3P Preliminary Risk Characterization Report," I3P Research Report. 2006.
- [3] C. Beaver, R. Schroepel, and L. Snyder, "A Design for Anonymous, Authenticated Information Sharing," from the Proc. 2001 IEEE Workshop on Information Assurance and Security.